On the Formal Verification of Optical Quantum Gates in HOL

Mohamed Yousri Mahmoud[1(✉)], Prakash Panangaden[2], and Sofiène Tahar[1]

[1] Electrical and Computer Engineering Deptartment, Concordia University, Montreal, Canada
{mo_solim,tahar}@ece.concordia.ca
http://hvg.ece.concordia.ca
[2] Computer Science Department, Mcgill University, Montreal, Canada
prakash@cs.mcgill.ca

Abstract. Quantum computers are expected to handle hard computational problems and provide unbreakable security protocols. Among different quantum computer implementations, those based on quantum optics and nuclear magnetic resonance show good advancement in building large scale machines. However, the involvement of optical and nuclear techniques makes their development very critical. This motivates us to apply formal techniques, in particular theorem proving, in quantum circuits analysis. In this work, we present the formalization of multi-inputs/multi-outputs quantum gates (technically called multi-modes optical circuits). This requires the implementation of tensor product over complex-valued functions. Firstly, we build a formal model of single optical beams and then extend it to cover circuits of multi optical beams, with the help of the developed tensor product algebra. As an application, we formally verify the behavior of the optical quantum CNOT gate and Mach-Zehnder interferometer.

Keywords: Quantum computing · Multi-modes · Tensor product · CNOT gate · Mach-Zehnder · Theorm proving · HOL light

1 Introduction

Quantum computers implemnt algorithms that would outperform classical machines, in particular for solving hard problems: a well known example is Shor's algorithm for integer factorization [10]. The new machine capabilities also offer powerful unbreakable security systems, e.g., [2]. Similar to classical machines, quantum ones consist of a new notion of a bit, called quantum bit (abbreviated as *qbit*), and a set of universal quantum gates, e.g., the Controlled NOT (the quantum counterpart of the classical NOT gate) [18]. The implementation of the quantum machine has been carried out in small scales using different means and technologies, such as ion traps [6] and quantum dots [11]. Many efforts are being invested for large scale machines [9], where optical circuits with the help of *Nuclear Magnetic Resonance* [20] and *Optical Nuclear Coupling* [7] are more reliable to implement such large scale computers.

M. Núñez and M. Güdemann (Eds.): FMICS 2015, LNCS 9128, pp. 198–211, 2015.
DOI: 10.1007/978-3-319-19458-5_13

The analysis and verification of this kind of optical quantum circuits and gates is very critical and faces some difficulties since traditional analysis techniques are ineffective. For instance, it has been proved that the simulation of a single time instance of a quantum system requires solving an exponential number of differential equations [4]. This motivates us to apply formal methods in this area, since the latter has enabled significant advancements took place in many engineering areas, e.g., analog systems designs [22], information theory [17], and sensor networks [3].

Recently, some developments for the formal verification of quantum optics has been conducted in higher-order logic (HOL) theorem proving [12] [14]. The main reason behind the choice of HOL is because of the high expressiveness it offers. Definitely, this comes at the expense of the full automation that HOL provers do not offer. However, HOL theorem proving still provides a good compromise compared to other automated formal techniques, such as model checking [1], that are unable to deal with the details of quantum systems. The application of abstraction techniques is not of much help as it would implicitly converge a quantum system to a classical one [21]. Frst-order logic is not suitable either since in most of the targeted quantum definitions and theorems there are quantifications over functions and predicates.

Based on [14], the formal model of one of the quantum computer gates, namely the optical flip gate, has been developed along with its verification [13]. However, the existing work is limited to single-input/single-output optical systems, which is technically called the single-mode optical beams theory. In this paper, we tackle the formalization of tensor product for complex-valued functions in order to allow the analysis of multi-inputs/multi-outputs systems, which is technically called multi-mode optical beams theory. As an application, we apply the multi-mode theory in the analysis of two quantum optical circuits: the Mach-Zehnder interferometer [16] and the Controlled NOT gate [19]. The former is a common circuit in quantum computing and quantum optics. The latter is a larger circuit, which is one of the universal gates of quantum computers. This shows the effectiveness of formal methods, especially in the case of complicated circuits with multiple connections. The verification of the two circuits is handled by two tactics that automatize most of the process, which removes a lot of burden from the interactive user, typically a system designer.

The rest of the paper is organized as follows: Section 2 briefly summarizes some basics of quantum optics. Section 3 deals with the formalization of L^2 space and single-mode theory. Section 4 contains the formalization of multi-mode and tensor product. Then, Section 5 discusses the formalization of the CNOT gate and the Mach-Zehnder interferometer and their verification, along with more elaboration about the tactics involved. Finally, we conclude the paper in Section 6 and provide hints to future work.

Note: the whole formalization presented here is implemented using the HOL Light theorem prover, and is freely available at [15].

2 Background

Any physical system has a mathematical model that describes its *state*. In classical physics, a system state can be deterministically evaluated at any time. However, in quantum theory, a system state has a probabilistic nature. In other words, a *quantum state* of a system, written as $|\psi\rangle$ [5], acts as a probability density function. Accordingly, the system state should satisfy the normalization condition (i.e., its integration over the real line is equal to one). In particular, in quantum optics theory, a state of an optical beam $\psi(q)$ is of type *real* $\rightarrow$ *complex* and satisfy the following condition:

$$\int_{-\infty}^{\infty} \psi^*(q)\ \psi(q)dq = 1 \tag{1}$$

where q, in some physics interpretations, refers to the electric charges inside the optical beam [16].

A collection of such quantum states forms an inner product space, equipped with the Lebesgue integral as the inner product function. Formally, the inner product of two quantum states f and g is denoted as $\langle f|g\rangle$, and it is equal to $\int_{-\infty}^{\infty} f^*(q)\ g(q)dq$. A major consequence of this mathematical formalization of an optical beam is the consideration of light as a stream of particles, called photons, instead of the ray or wave nature as was believe in the classical theory.

Since quantum states form a linear function space, then there exists an infinite basis that spans such a space. In case of an optical beam, so-called *fock states* form the basis states, i.e., any $|\psi\rangle$ can be written as follows:

$$|\psi\rangle = \sum_n c_n \left|n\right\rangle$$

where c_n's are complex numbers such that $\sum_n c_n = 1$, and $\left|n\right\rangle$ is a fock state representing the existence of n photons inside the optical beam. Note that $\left|0\right\rangle$ is called the vacuum state, and describes the case of zero photons.

For a fock state, we are interested in a number of operations. An operator $\hat{a}$ is called the *annihilation* operator and another operator written $\hat{a}^\dagger$ is called the *creation* operator. These operators are adjoints of each other, i.e., $\langle \hat{a}\ n_1|n_2\rangle = \langle n_1|\hat{a}^\dagger\ n_2\rangle$, and their commutation is equal to 1, i.e., $\hat{a}\ **\ a^\dagger - \hat{a}^\dagger\ **\ \hat{a} = I$ (note that I is the unity function, and the multiplication $**$ is point-wise multiplication). The effect of these operators on fock states is described as follows:

$$\hat{a}\left|n\right\rangle = \sqrt{n}\left|n-1\right\rangle \text{ and } \hat{a}^\dagger\left|n\right\rangle = \sqrt{n+1}\left|n+1\right\rangle. \tag{2}$$

Another important operator is the *number operator* $\hat{N} = \hat{a}^\dagger\ **\ \hat{a}$, which returns the number of photons:

$$\hat{N}|n\rangle = n * |n\rangle$$

This shows that fock states are eigenvectors of the number operator.

Based on photon number operator, we can define the energy operator $\hat{H} = \frac{1}{2}\hbar\omega(\hat{N}+I)$, where ω is called the mode resonance frequency and $\hbar$ is the planck

constant. The operator returns the amount of energy in a light beam. This formalization of energy inside an optical beam leads to the existence of energy in the vacuum state, i.e., in the absence of photons, the main source of energy in a beam. This is one of the interesting results in the quantum paradigm that does not have a classical counterpart.

All the above mentioned definitions, formulas and equations form the single-mode optical beams theory. This theory is suitable as long as we are dealing with systems that involve no more than one single beam. In order to tackle more general systems with multiple optical beams, we should consider the theory of multi-modes. The core idea is how to consider two independent optical beams (or particles), given that one has the individual physical description of each. For this purpose, we utilize the mathematical tool of tensor product. Let us assume the existence of two beams with quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$, then we have a new quantum state $|\psi_1 \otimes \psi_2\rangle$ that describes both beams simultaneously. The new state satisfies the following properties:

$$|c * \psi_1 \otimes \psi_2\rangle = c * |\psi_1 \otimes \psi_2\rangle \text{ and}$$

$$|\psi_1 + \psi_2 \otimes \psi_3\rangle = |\psi_1 \otimes \psi_3\rangle + |\psi_2 \otimes \psi_3\rangle$$

For this kind of states, we need to develop suitable operators based on the existing ones. For instance, for two annihilation operators we will have a new tensor product operator $\hat{a}_1 \otimes \hat{a}_2$, where subscripts refer to the modes to which they belong. This operator when it is applied to $|\psi_1 \otimes \psi_2\rangle$, results in $|\hat{a}_1\psi_1 \otimes \hat{a}_2\psi_2\rangle$. It also satisfies similar properties such as tensor product of states, e.g., $(\hat{a}_1^\dagger + \hat{a}_1) \otimes \hat{a}_2^\dagger = \hat{a}_1^\dagger \otimes \hat{a}_2^\dagger + \hat{a}_1 \otimes \hat{a}_2^\dagger$.

In the following sections, we will present the formal aspects of the theories presented in Section 2, where we elaborate more on the details of the higher-order logic implementation.

3 Single-Mode Formalization

As we described in Section 2, the set of quantum states lies in the inner product space of square Lebesgue integrable functions. In [14], the quantum states space was defined axiomatically as an inner product space of the functions of type `A` $\longrightarrow$ `complex`. In this formalization, we instantiate `A` to be `real`, since the electric charge q is of type real. Thus, we define a new type `bqs` : `real` $\longrightarrow$ `complex` which stands for `b`eam `q`uantum `s`tate. Based on the new type, we can then define the notion of space of complex-valued square integrable functions L^2.

We start by formally defining the notion of the set of square integrable complex-valued functions, namely `sq_integrable`:

Definition 1.

```
new_specification ["sq_integrable"]
  ∀f. f ∈ sq_integrable ⇔
1     f complex_measurable_on (: real) ∧
2     (λx. ||f x|| ²) real_integrable_on (: real)
```

Since we are dealing with complex-valued functions then the square of a function `f` means the multiplication of `f(x)` by its conjugate $\texttt{f(x)}^*$. This is equivalent to the norm square of `f(x)`, as presented in Line 2. There is another mandatory condition to form a subspace of these functions, which is the complex measurability [8]:

Definition 2.

```
f complex_measurable_on s ⇔
  (λx. Re (f x)) real_measurable_on s ∧
    (λx.Im (f x)) real_measurable_on s
```

Note here that the measurability and integrability are over the whole real line (i.e., from $-\infty$ to ∞). We refer the reader to [8], where more information about measure theory can be found. Next, we define the inner product function over the elements of space `sq_integrable` as follows:

Definition 3.

```
r_inprod f g =
1  complex(real_integral (: real) (λx : real. Re((f x)* ∗ (g x))),
2  real_integral (: real) (λx.Im ((f x)* ∗ (g x))))
```

The above definition states that the inner product of two square integrable functions `f` and `g` is a complex value, whose real part is the real integral of the real part of `f ∗ g` (see Line 1), and its imaginary part is the real integral of the imaginary part of `f ∗ g` (see Line 2).

Now, we move to the most important step, namely to prove that these definitions form a linear space and the associated `r_inprod` function is its inner product. Formally, we need to prove the following set of properties according to [12]:

Theorem 1.

```
is_cfun_subspace sq_integrable ∧ ∀x. x ∈ sq_integrable ⇒
real (r_inprod x x) ∧ 0 ≤ real_of_complex (r_inprod x x) ∧
(r_inprod x x = Cx(0) ⇔ x = cfun_zero) ∧
∀y. y ∈ sq_integrable ⇒ cnj (r_inprod y x) = r_inprod x y ∧
(∀a. r_inprod x (a%y) = a ∗ (r_inprod x y)) ∧
∀z. z ∈ sq_integrable ⇒ r_inprod (x + y) z = r_inprod x z + r_inprod y z
```

where `cfun_zero` is a function that always returns zero regardless of the input parameter, `%` refers to scalar multiplication.

The proof details of above theorem is complex and outside the scope of the paper. We refer interested readers to [15] for proof scripts, where they can find more details. According to the above shown properties, we can prove the following result, which is a conjunction of them:

Theorem 2.
`is_inner_space (sq_integrable, r_inprod)`

Now, we have all ingredients to formally implement the single-mode (see Section 2):

Definition 4.
`is_sm sm` $\Leftrightarrow$ `0 < w sm` $\wedge$
1 `is_hermitian(sq_integrable, r_inprod) (anh sm)(cr sm)`
2 $\wedge$ `anh sm com cr sm = I` $\wedge$ `is_qst (vac sm)`
3 `is_eigen_pair (h sm) (vac sm, Cx(planck *` $\frac{\texttt{(w sm)}}{2}$`))`

where a single-mode `sm` consists of the creator `cr`, annihilator `anh`, resonance frequency `w` and vacuum state `vac`. Line 1 assumes the adjointness between creator and annihilator, where `is_hermitian` is defined as follows:

Definition 5.
`is_hermitian (s, inprod) op`$_1$ `op`$_2$ $\Leftrightarrow$
`is_inner_space (s, inprod)` $\Rightarrow$
$\forall$`x y. inprod x (op`$_2$ `y) = inprod (op`$_1$ `x) y`

Line 2 in Definition 4 assumes the commutation between the same operators and Line 3 assumes the relation between the vacuum state and the energy operator, where `is_eigen_pair` is defined as follows:

Definition 6.
`is_eigen_pair op (v,` μ`)` $\Leftrightarrow$
`op v =` μ`% v` $\wedge$ `(v` $\neq$ `cfun_zero)`

Recall that a single-mode field at a fock state $|n\rangle$ means that the light stream contains exactly n photons. Such states are quite important since they form the basis of the single-mode quantum states space. Accordingly, we define fock states as follows:

Definition 7.
`fock sm 0 = vac sm` $\wedge$
`fock sm (SUC n) = get_qst(cr sm (fock sm n))`

where `get_qst f` $= \sqrt{\texttt{r\_inprod f f}}$ `% f`, i.e., returns the normalized version of a square integrable function, which is typically a quantum state.

For the given definition of the fock state, we prove the effect of creator and annihilator on fock states as presented in Section 2:

Theorem 3.
$\forall$`n sm.is_sm sm` $\Rightarrow$
`(cr sm) (fock sm n) = Cx(sqrt((SUC n)))%fock sm (SUC n)` $\wedge$
$\Rightarrow$ `(anhhsm) (fock sm (SUC n)) =` $\sqrt{\texttt{SUC n}}$ `% fock sm n`

In the next section, we will present the multi-mode formalization which is the main tool, in addition to single-mode, to formally verify the CNOT gate and the Mach-Zehnder interferometer.

4 Multi-Mode Formalization

The core idea of the Multi-Mode formalization is based on the development of the tensor product between states and operators. Before we present the general definition of quantum states tensor product, we will show an example of the tensor product of only two states. Given a quantum state $|n_1\rangle$ of an optical beam, in one of the interpretations of quantum mechanics, this state (i.e., the complex valued functions) is a probability density function which provides the probability of the number of photons inside the optical beam. Now, if we have another beam with state $|n_2\rangle$, the function that describes the joint probability of the two beams is the point-wise multiplication of $|n_1\rangle$ and $|n_2\rangle$. Hence, we define the tensor product of two quantum states as follows: $\lambda y_1\ y_2.\ |n_1\rangle\ y_1 * |n_1\rangle\ y_2$. To generalize for n beams, we define the tensor product recursively as follows:

Definition 8.

$$\begin{aligned}&\texttt{tensor 0 (modes : bqs}^{\texttt{N}}\texttt{)} = \texttt{K(Cx(1))} \wedge \\ &\quad \texttt{tensor (SUC n) (modes)} = \\ &\qquad (\lambda \texttt{y} : \texttt{A}^{\texttt{N}}.((\texttt{tensor n modes})\ \texttt{y}) * (\texttt{modes\$(SUC n)})\ (\texttt{y\$(SUC n)}))\end{aligned}$$

where `modes` is a vector of size n that contains n modes. The base case of the zero modes is a trivial case; it only guarantees a terminating definition. We then define the tensor product of operators as follows:

Definition 9.

$$\begin{aligned}&\texttt{is\_tensor(tens : cops}^{\texttt{N}} \longrightarrow (\texttt{real}^{\texttt{N}} \longrightarrow \texttt{complex}) \longrightarrow (\texttt{real}^{\texttt{N}} \longrightarrow \texttt{complex})) \Rightarrow \\ &\quad \forall(\texttt{ops} : (\texttt{bqs} \longrightarrow \texttt{bqs})^{\texttt{N}})\ (\texttt{modes : bqs}^{\texttt{N}})\ \texttt{n.}\ \texttt{is\_linear\_cop}\ (\texttt{tens ops}) \wedge \\ &\quad \texttt{tens ops}\ (\texttt{tensor n modes}) = \texttt{tensor n(lambda i.(ops\$i)}\ (\texttt{modes\$i}))\end{aligned}$$

where `ops` is a vector of operators defined on the single-modes, and `tens ops` is the tensor product. Note that the resulting new operator is only applicable to the tensor product of states. That is why we define it in a predicate form in order to restrict its functionality. For this definition, we prove the following crucial property of the operators tensor product, associativity:

Theorem 4.

$$\begin{aligned}&\forall\ \texttt{ten ops1 ops2 n modes.} \\ &\quad \texttt{is\_tensor ten} \Rightarrow \texttt{ten ops2(ten ops1 (tensor nmodes))} = \\ &\quad \texttt{ten}\ ((\lambda\ \texttt{i.}\ (\texttt{ops2\$i})\ \texttt{o}\ (\texttt{ops1\$i})))\ (\texttt{tensor n modes})\end{aligned}$$

where `o` refers to function composition.

As we will see later, an optical quantum circuit accepts single-modes as inputs, however, the circuit operation itself runs in multi-mode. Thus, we need to develop a function to embed (or express) a single-mode operator in a multi-mode fashion. For this purpose, we define the following function:

Definition 10.

$$\begin{aligned}&\texttt{pos}\ (\texttt{tens : cops}^{\texttt{N}} \longrightarrow (\texttt{A}^{\texttt{N}} \longrightarrow \texttt{complex}) \longrightarrow (\texttt{A}^{\texttt{N}} \longrightarrow \texttt{complex}))\ (\texttt{op : cops})\ \texttt{m} = \\ &\quad \texttt{tens}\ (\texttt{lambda i. if i} = \texttt{m then op else I})\end{aligned}$$

The concept of `pos` (or positioning) is to place a given operator in a specific mode (based on its order in the input list) and leave the other modes with the identity operator. Now, we will utilize the development of multi-mode to define a very important optical element, of which many quantum circuits are built.

Beam Splitter in Multi-Mode

A beam splitter is a device that takes a beam of light and partly transmits it and partly reflects it, thus splitting the beam into two beams. The remarkable feature of quantum mechanics is that a *single photon* can be split by a beam splitter.

In its standard definition, a beam splitter consists of two-input/two output ports. We can recognize each port (or optical mode) by the creator and annihilator operators, as shown Figure 1:

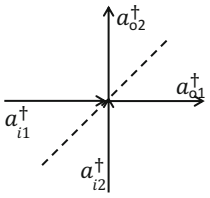

Fig. 1. Beam Splitter- Standard Inputs and Outputs

The beam splitter then relates input modes with the output modes according to the following matrix representation:

$$\begin{pmatrix} \hat{a}^\dagger_{o1} \otimes I \\ I \otimes a^\dagger_{o2} \end{pmatrix} = \begin{pmatrix} \mathbf{T}' & \mathbf{R} \\ \mathbf{R}' & \mathbf{T} \end{pmatrix} \begin{pmatrix} \hat{a}^\dagger_{i1} \otimes I \\ I \otimes a^\dagger_{i2} \end{pmatrix} \tag{3}$$

with the following relations between the coefficients :

$$|\mathbf{R}'| = |\mathbf{R}|,\ |\mathbf{T}'| = |\mathbf{T}|,\ |\mathbf{R}|^2 + |\mathbf{T}|^2 = 1,$$

$$\mathbf{R}^*\mathbf{T}' + \mathbf{R}'\mathbf{T}^* = 0, \text{ and } \mathbf{R}^*\mathbf{T} + \mathbf{R}'\mathbf{T}'^* = 0.$$

These coefficients are of type complex and represent the reflectivity and transitivity in some sense. We now have the quantum mechanical description of the beam splitter, and thus we can develop its formal version as follows:

Definition 11.

```
1 is_beam_splitter(p1, p2, p3, p4, ten, i1, m1, i2, m2, o1, m3, o2, m4) ⇔
2   is_sm i1 ∧ is_sm i2 ∧ is_sm o1 ∧ is_sm o2
3   ∧ w i1 = w i2 ∧ w i2 = w o1 ∧ w o1 = w o2 ∧
4   vac i1 = vac i2 ∧ vac i2 = vac o1 ∧ vac o1 = vac o2 ∧
5   pos ten (cr i1) m1 = p1*% pos ten (cr o1) m3 + p2*% pos ten (cr o2) m4
6   pos ten (cr i2) m2 = p3*% pos ten (cr o1) m3 + p4*% pos ten (cr o2) m4
```

Note that the formal definition of beam splitters relates the inputs operators in terms of the outputs operators (see Line 5 and Line 6), to the contrary of the theoretical definitions presented earlier in Equation (3): This form is practical for the analysis of the circuits, as we will see later, since the goal is to generate the output states from the input states. Thus, the parameters {`p1,p2,p3,p4`} are the inverse of the matrix presented before. In Line 1, the parameters {`m1,m2,m3,m4`} define the order of each mode in the whole circuit. In the case of a circuit of only two inputs/two outputs, the possible values of these parameters are 1 and 2. Line 2 and Line 3 ensure that the four modes are proper single modes, and working with the same frequency and vacuum state (i.e., the state of zero photons).

Now, we have the full tools to tackle any circuit that consists of beam splitters, and generate the corresponding output of this circuit.

5 Quantum Optical CNOT Gate

In this section, we will tackle the formalization of the universal quantum CNOT gate. Before this step, we will study the formalization of a simpler circuit, namely *Mach-Zehnder* Interferometer, in order to illustrate how the mathematics work in these kind of circuits, which also applies for the larger circuits, e.g., the CNOT gate.

5.1 Mach-Zehnder Verification

The most interesting use of the beam splitter is to combine it with mirrors that reflect the incident photon. The configuration shown in Figure 2 is called a *Mach-Zehnder* Interferometer. There are two beam splitters labelled BS_1 and BS_2. The grey objects shown are mirrors. The photon is shown as a wavy line. The photon incident at BS_1 is split in the manner we have described above, where each beam splitter is working according the matrix $\frac{1}{\sqrt{2}}\begin{pmatrix} -i & 1 \\ -1 & i \end{pmatrix}$, and each mirror produces phase shifts of i over creation operators.

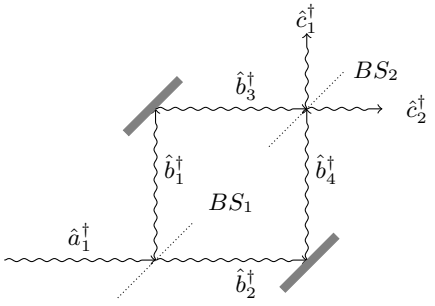

Fig. 2. Mach-Zehnder Interferometer- Inputs and Outputs

Accordingly, we have the following transformation between the different creations operators:

$$\begin{aligned}
\mathbf{a}_1^\dagger &= \tfrac{1}{\sqrt{2}}(i\mathbf{b}_1^\dagger + \mathbf{b}_2^\dagger)\\
\mathbf{b}_1^\dagger &= i\mathbf{b}_3^\dagger\\
\mathbf{b}_2^\dagger &= i\mathbf{b}_4^\dagger\\
\mathbf{b3}_1^\dagger &= \tfrac{1}{\sqrt{2}}(i\mathbf{c}_1^\dagger + \mathbf{c}_2^\dagger)\\
\mathbf{b4}_1^\dagger &= \tfrac{1}{\sqrt{2}}(\mathbf{c}_1^\dagger + i\mathbf{c}_2^\dagger)
\end{aligned}$$

Given that only one photon incidents at the input mode $\mathbf{a}_1^\dagger$(see Figure 2), then the state of the input modes is $|1\rangle \otimes |0\rangle$. According to Equation (2), this is equal to $\mathbf{a}_1^\dagger \otimes I(|0\rangle \otimes |0\rangle)$. Carrying out the above transformations of the field operators all the way to the end, the output modes state becomes equal to $i\mathbf{c}_1^\dagger \otimes I(|0\rangle \otimes |0\rangle)$, i.e., the photon will leave from the vertical port of BS_2 (see Figure 2). In the following, we see how to formally prove this result along with the formal definition of the Mach-Zehnder interferometer.

Before we present the theorem that verifies the above result, we have to define the notion of mirror, similar to what we have for the beam splitters:

Definition 12.

```
mirror(ten, i1, m1, o1, m2) ⇔
  pos ten(cr i1) m1 = i % pos ten (cr o1) m2
```

The following theorem shows the formal structure of the above circuit, and proves that if we receive a photon at the horizontal input of the interferometer, then it will leave at the vertical output of the interferometer:

Theorem 5.

```
 ∀a b d.
   is_tensor ten∧
1   is_beam_splitter (−√(1/2) ∗ ii, √(1/2)), −√(1/2), √(1/2) ∗ ii,
      ten, a$1, 1, a$2, 2, b$1, 1, b$2, 2)∧
2   mirror(ten, b$1, 1, b$3, 1) ∧ mirror(ten, b$2, 2, b$4, 2)∧
3   is_beam_splitter (−√(1/2) ∗ ii, √(1/2)), −√(1/2), √(1/2) ∗ ii,
      ten, b$3, 1, b$4, 2, c$1, 1, c$2, 2)
4    ⇒ tensor 2 (lambda i. if i = 1 then fock (a$1) 1 else vac) =
5      ii% tensor 2 (lambda i. ifi = 1 then fock (c$1)1 else vac)
```

Lines (1-3) provide the structure of the circuit in Figure 2 with the same modes naming. Line 4 describes the input modes, where we have one photon at mode $\mathbf{a}_1^\dagger$ and nothing elsewhere. Line 5 provides the corresponding output modes, where we obtain one photon at mode $\mathbf{c}_1^\dagger$ and nothing elsewhere.

Now, we will move to a more complex circuit, where we will focus on the formal results obtained rather than the proof steps.

5.2 CNOT Gate Verification

Similar to classical computer, the basic component of the quantum computer is the quantum bit (or *qbit*). A quantum bit is a quantum system with two basis states $|0\rangle$ and $|1\rangle$. However, in contrast to its classical counterpart, the state of a qbit is not only $|0\rangle$ or $|1\rangle$, but can be a mix. Indeed, such a state can be expressed as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. There are a number of operations that can be defined over these qbits. In this paper, we are interested in the Controlled NOT gate. It is a two inputs/two outputs gate, namely *control* and *target* signals. The gate semantic is to invert the target bit whenever the control bit is equal to one, and nothing changes as long as the control bit is equal to zero. The control bit is always transmitted as is. In other word: if the possible input is $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \eta|11\rangle$ then the output is $|\psi_o\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \eta|10\rangle$.

In quantum optics, this gate can be implemented using five beam splitters [19], as given in Figure 3, where each of the control and target qbits is repre-

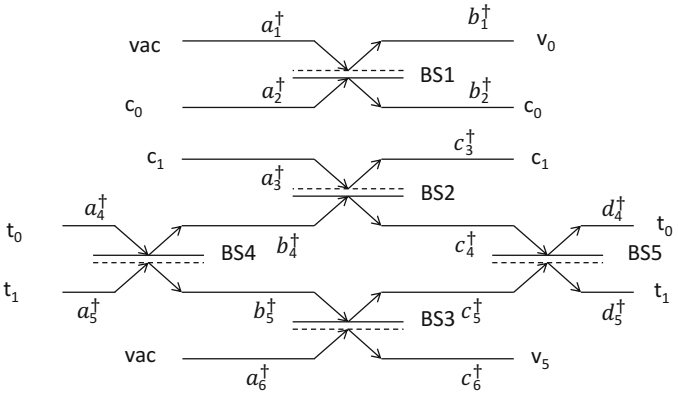

Fig. 3. Controlled NOT gate optical implementation

sented using two optical beams, and each of the beam splitter follows the matrix $\begin{pmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ \sqrt{1-\eta} & -\sqrt{\eta} \end{pmatrix}$. For BS4, BS5 η is equal to $\frac{1}{2}$, and for the rest it is equal to $\frac{1}{3}$. The encoding of such four beams is as follows: applying a single photon to c_0 is equivalent to setting the control bit to zero, and applying the photon to c_1 is equivalent to setting the control bit to one (same rule applies for the target bit). In Figure 3, *vac* refers to vacuum state, i.e., we do not apply any photons at these ports. For the output modes, v_0 and v_5 are dummy signals and do not have any semantic.

Now the formal definition of such circuit is included in the following theorem:

Theorem 6.

$\forall$a b c d.
  is_tensor ten $\wedge$
1 is_beam_splitter $(\sqrt{\frac{1}{3}}, \sqrt{\frac{2}{3}}, \sqrt{\frac{2}{3}}, -\sqrt{\frac{1}{3}}, \texttt{ten}, \texttt{a\$2}, 2, \texttt{a\$1}, 1, \texttt{b\$2}, 2, \texttt{b\$1}, 1) \wedge$
2 is_beam_splitter$(\sqrt{\frac{1}{2}}, \sqrt{\frac{1}{2}}, \sqrt{\frac{1}{2}}, -\sqrt{\frac{1}{2}}, \texttt{ten}, \texttt{a\$4}, 4, \texttt{a\$5}, 5, \texttt{b\$4}, 4, \texttt{b\$5}, 5) \wedge$
3 is_beam_splitter$(\sqrt{\frac{1}{3}}, \sqrt{\frac{2}{3}}, \sqrt{\frac{2}{3}}, -\sqrt{\frac{1}{3}}, \texttt{ten}, \texttt{b\$4}, 4, \texttt{a\$3}, 3, \texttt{c\$4}, 4, \texttt{c\$3}, 3) \wedge$
4 is_beam_splitter$(\sqrt{\frac{1}{3}}, \sqrt{\frac{2}{3}}, \sqrt{\frac{2}{3}}, -\sqrt{\frac{1}{3}}, \texttt{ten}, \texttt{b\$5}, 5, \texttt{a\$6}, 6, \texttt{c\$5}, 5, \texttt{c\$6}, 6) \wedge$
5 is_beam_splitter$(\sqrt{\frac{1}{2}}, \sqrt{\frac{1}{2}}, \sqrt{\frac{1}{2}}, -\sqrt{\frac{1}{2}}, \texttt{ten}, \texttt{c\$4}, 4, \texttt{c\$5}, 5, \texttt{d\$4}, 4, \texttt{d\$5}, 5) \Rightarrow$
6 $|010100\rangle = \frac{1}{3} * (\underline{|010100\rangle} + \sqrt{2} * |101000\rangle$
7 $+ \sqrt{2} * |100001\rangle + |011000\rangle + |010001\rangle + \sqrt{2} * |100100\rangle)$

Lines (1-5) represent the formal structure of the CNOT gate in Figure 3. Note that we used the bra-ket notation [5] in the formal theorem for simplicity, in the actual code all states are written the same form as in the Mach-Zehnder example (see Theorem 5). The order of the output bits, on the right hand side of Line 6 and Line 7, is $v_0, c_0, c_1, t_0, t_1, v_5$.

According to [19], the output of the circuit in Figure 3 is not exactly as desired: As one can notice from Line 6 and Line 7, in the case of the control bit is equal to zero and the target bit is equal to zero. The result on the right hand side contains many possibilities of different probabilities, among them the required (underlined) one with probability $(\frac{1}{3})^2$. Note that these unwanted possibilities do not contain at all any meaningful states, i.e., $|011000\rangle$, $|001100\rangle$, $|001010\rangle$. We can get rid of these unwanted outputs by a physics process called coincidence basis [19]. We also verify the case where the control gate is equal to zero and the target is equal to one. The result was compatible with the one presented in [19]. Similarly, we verified the case of the control is equal to one. For example in case of $|001100\rangle$, the following theorem shows the result:

Theorem 7.

$\texttt{tensor}\ |001100\rangle = \frac{1}{3} * (|001010\rangle - \sqrt{2} * |002000\rangle - |001001\rangle +$
  $\sqrt{2} * |000200\rangle + |000101\rangle + |000110\rangle + |000011\rangle)$

The formal analysis of these two optical circuits would not have been possible without the development of the following tactic: `MULTI_MODE_DECOMPOSE_TAC` which is responsible for passing the creator operator in/out to/from the different modes. As its name suggests, it acts like decomposing multi-modes to many single modes that can be dealt with using the single-mode theorems.. The key lemma, on which this tactic is built, is:

Theorem 8.

$\forall$p q f x.(p x $\Rightarrow$ f x = q) $\Rightarrow$ (if p x then q else (f x)) = f x

This lemma typically reduces multi-mode to single-mode, whenever all possible conditions (in the `if` statement) reduce to the same predicate.

Besides above tactic, we have developed a few other, such as `CFUN_FLATTEN_TAC`, which takes the whole formula to complex level, at final stage of the proof, to handle some algebraic simplification to finalize the proof. Without these tactics the verification of Mach-Zehnder and CNOT would be lengthly and complicated. Interested readers can check the HOL script of these tactics at [15], and see how they are utilized in the proofs.

This interesting result concludes the whole formalization by showing the effectiveness of formal methods, in particular with large circuits with a large number of connections and variables. Note that this circuit is working on 6 modes in each step, with the actual number of single modes (including intermediates) equal to 16.

6 Conclusion

Quantum computers are expected to outperform classical machines in certain cases, and provide powerful and unbreakable security systems. Among many implementations, quantum optical circuits with the help of nuclear optical coupling and nuclear magnetic resonance showed good advancement in building quantum machines at large scale. Thus, the quantum computer development became very critical. In this paper, we have studied the applicability of formal methods, in particular of HOL theorem proving, for the formal analysis and verification of quantum optical computers. The presented work includes the formalization of optical single-mode and multi-mode that helped in the analysis of quantum gates. As an illustrative application, we presented the verification of the Mach-Zehnder interferometer and Controlled NOT gate. Throughout our development, we have experienced a number of difficulties. We had a problem to find one clear definition of many quantum concepts. Physics books present the same idea from different perspectives and each considers some implicit assumptions. To deal with this problem, we focused our axiomatic definitions on the common ground of the different physics resources. The usability and readability of definitions and theorems are another challenge, where in the first versions of our development, we had lengthy definitions and theorems due to the high number of variables that control the quantum process. For this situation, we tried to remove irrelevant variables (which is a kind of low-level abstraction) that do not affect the quantum natures of systems. We also enhanced the proving process by developing dedicated tactics. This facilitates the reasoning about potentially similar circuits and gates and removes the burden of tedious steps, in particular with large circuits that have a high number of modes (i.e., optical beams). As a future work, we are targeting the formalization of more complicated quantum gates, e.g., the Hadamard gate [19], and enhancing the whole verification process to be more automated.

References

1. Baier, C., Katoen, J.P.: Principles of Model Checking. MIT Press (2008)
2. Brassard, G., Crepeau, C., Jozsa, R., Langlois, D.: A quantum bit commitment scheme provably unbreakable by both parties. In: Proceedings IEEE Annual Symposium on Foundations of Computer Science, pp. 362–371 (1993)
3. Elleuch, M., Hasan, O., Tahar, S., Abid, M.: Towards the formal performance analysis of wireless sensor networks. In: Proceedings IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises, pp. 365–370 (2013)
4. Feynman, R.: Simulating physics with computers. International Journal of Theoretical Physics 21, 467–488 (1982), doi:10.1007/BF02650179
5. Griffiths, D.J.: Introduction to Quantum Mechanics. Pearson Prentice Hall (2005)
6. Haeffner, H., Roos, C.F., Blatt, R.: Quantum computing with trapped ions. Physics Reports 469(4), 155–203 (2008)
7. Jones, J.A.: Quantum computing: Optical nuclear coupling. Natural Photonics 5(11), 513 (2011)
8. Kolmogorov, A.N., Fomin, S.V., Fomin, S.V.: Elements of the Theory of Functions and Functional Analysis. Dover books on mathematics, vol. 2. Dover (1999)
9. Ladd, T.D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., O'Brien, J.L.: Quantum computers. Nature 464, 45–53 (2010)
10. Lomonaco, S.J.: Quantum Computation: A Grand Mathematical Challenge for the Twenty-first Century and the Millennium. American Mathematical Society (2002)
11. Loss, D., DiVincenzo, D.P.: Quantum computation with quantum dots. Physical Review A 57, 120–126 (1998)
12. Mahmoud, M.Y., Aravantinos, V., Tahar, S.: Formalization of infinite dimension linear spaces with application to quantum theory. In: Brat, G., Rungta, N., Venet, A. (eds.) NFM 2013. LNCS, vol. 7871, pp. 413–427. Springer, Heidelberg (2013)
13. Mahmoud, M.Y., Aravantinos, V., Tahar, S.: Formal verification of optical quantum flip gate. In: Klein, G., Gamboa, R. (eds.) ITP 2014. LNCS, vol. 8558, pp. 358–373. Springer, Heidelberg (2014)
14. Mahmoud, M.Y., Tahar, S.: On the quantum formalization of coherent light in HOL. In: Badger, J.M., Rozier, K.Y. (eds.) NFM 2014. LNCS, vol. 8430, pp. 128–142. Springer, Heidelberg (2014)
15. Mahmoud, M.Y.: Formal verification of optical quantum gates - HOL Light script (2014), http://hvg.ece.concordia.ca/code/QGates/
16. Mandel, L., Wolf, E.: Optical Coherence and Quantum Optics. Cambridge University Press (1995)
17. Mhamdi, T., Hasan, O., Tahar, S.: Formalization of entropy measures in HOL. In: Interactive Theorem Proving. LNCS, vol. 6898, pp. 233–248. Springer, Heidelberg (2011)
18. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press (2010)
19. Ralph, T.C., Langford, N.K., Bell, T.B., White, A.G.: Linear optical controlled-not gate in the coincidence basis. Physics Review A 65, 062324 (2002)
20. Verhulst, A.S.: Optical pumping experiments to increase the polarization in nuclear-spin based quantum computers. PhD thesis, Stanford University, CA, USA (2004)
21. Yamashita, S., Markov, I.L.: Fast equivalence-checking for quantum circuits. In: IEEE/ACM International Symposium on Nanoscale Architectures, pp. 23–28 (2010)
22. Zaki, M.H., Tahar, S., Bois, G.: Formal verification of analog and mixed signal designs: A survey. Microelectronics Journal 39(12), 1395–1404 (2008)